



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/309,412	05/10/1999	KAZUHIRO HARA	450100-4879	7480

20999 7590 09/12/2003
FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER
JACKSON, JENISE E
ART UNIT 2131
PAPER NUMBER
DATE MAILED: 09/12/2003

8

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/309,412	HARA, KAZUHIRO
	Examiner Jenise E Jackson	Art Unit 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on ____.
 2a) This action is **FINAL**. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-36 is/are pending in the application.
 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
 5) Claim(s) ____ is/are allowed.
 6) Claim(s) 1-36 is/are rejected.
 7) Claim(s) ____ is/are objected to.
 8) Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on ____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 11) The proposed drawing correction filed on ____ is: a) approved b) disapproved by the Examiner.
 If approved, corrected drawings are required in reply to this Office action.
 12) The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. ____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
 * See the attached detailed Office action for a list of the certified copies not received.
 14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
 a) The translation of the foreign language provisional application has been received.
 15) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). ____ . |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) ____ . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-5, 8-14, 17-19, are rejected under 35 U.S.C. 102(b) as being anticipated by Seth-Smith et al.

3. As per claim 1, 11, a data transmission controlling method for controlling transmission of data from data transmitting means to data receiving means over communication channels (col. 3, lines 14-18, fig. 1, sheet 1), said data transmission controlling method includes, transmitting data encrypted by said data transmitting means to said data receiving means over a first communication channel provided for data transmission from said data transmitting means to said data receiving means (see col. 3, lines 14-22, fig. 1, sheet 1); and transmitting to said data receiving means restrictive data transmission control information for causing the encrypted data to be received solely by specific data receiving means (see col. 6, lines 30-49) at least over a second communication channel which, having a smaller capacity of data transmission than said first communication channel, is also used for data transmission from said data receiving means to said data transmitting means (see col. 6, lines 49-57, fig. 1, sheet 1). The Examiner asserts that Seth-Smith inherently discloses the second communication channel has a smaller capacity, because Seth-Smith discloses one channel can be a landline.

2. As per claim 2, wherein said second communication channel is a communication channel permitting bi-directional communication between said data transmitting means and said data receiving means, is inherent in Seth-Smith, because Seth-Smith discloses that the user can communicate with the broadcaster(see col. 6, lines 49-67).

3. As per claims 3, 12, wherein said data transmitting means performs data encryption using an encryption key and wherein said encrypted data from said data transmitting means are decrypted by said data receiving means utilizing a decryption key identical to said encryption key used in the data encryption(see col. 3, lines 23-27, col. 20, lines 22-34). The Examiner asserts that the keys must be identical in order to decrypt information, that insures that the proper individual receives information, this is disclosed in Seth-Smith et al.

4. As per claims 4, 13, Seth-Smith et al. discloses wherein said encryption key and said decryption key are session keys(i.e. service key) for encrypting and decrypting information and data(see col. 3, lines 14-22, col. 10, lines 38-42, col. 22, lines 9-36, 57-60).

5. As per claims 5, 14, Seth-Smith discloses wherein said session keys(i.e. service keys) are updated at predetermined intervals(see col. 11, lines 66-67, col. 12, lines 1-8, col. 19, lines 33-37).

6. As per claims 8, 17, Seth-Smith discloses said first communication channel is a satellite link permitting unidirectional communication from said data transmitting means to said data receiving means; and wherein said second communication channel is a communication channel permitting bi-directional communication between said data transmitting means and said data receiving means(see col. 6, lines 49-55).

7. As per claims 9-10, 18-19, Seth-Smith inherently discloses wherein said data receiving means is constituted as an IP router, and bridge, because Seth-Smith discloses a subscription television system that uses a satellite to transmit data(see abstract).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 6-7, 15-16, are rejected under 35 U.S.C. 103(a) as being unpatentable over Seth-Smith et al. in view of Mueller.

10. Seth-Smith discloses data transmitting means and said data receiving means, and discloses session keys(see above already addressed as per claim 1 and 4).

11. Seth-Smith et al. is silent on a master key that encrypts and decrypts session keys.

12. However, Mueller discloses a master key that encrypts and decrypts session keys(see col. 1, lines 46-61).

13. It would have been obvious to one ordinary skill in the art to combine the teachings of Mueller within the system of Seth-Smith, because secure session key generation methods, such as Mueller offer distinct advantage that the intercepted, encrypted messages based on the session key cannot be decrypted at a later time even if access to the actual encryption system is gained(see col. 2, lines 1-7 of Mueller).

Art Unit: 2131

14. As per claims 7, 16, Seth-Smith discloses said data transmitting means possesses said session keys corresponding to all data receiving means authorized to receive specific information and data; and wherein said data transmitting means transmits in advance said session keys to said data receiving means authorized to receive specific information and data(see col. 21, lines 49-65, col. 22, lines 9-34).

15. Claims 20-36 are rejected under 35 U.S.C. 102(b) as being anticipated by Aziz et al.

16. As per claim 20, Aziz et al. discloses a data transmission controlling method for controlling transmission of data from data transmitting means to data receiving means over communication channels(see col. 1, lines 64-67, col. 2, lines 1-5) and for causing said data transmitting means to encrypt data and transmit the encrypted data to said data receiving means over said communication channels(see col. 2, lines 9-25), said data transmission controlling method comprising the steps of encapsulating the data to be transmitted in multiplexed fashion in accordance with a plurality of protocols; and encrypting at least one of data capsules resulting from the encapsulation(see col. 2, lines 27-36).

17. As per claim 21, Aziz et al. discloses wherein the data encapsulating step, a first encapsulating step for encapsulating the data to be transmitted to said data receiving means in accordance with a first protocol(see col. 1, lines 64-67, col. 2, lines 1-5); and a second encapsulating step for further encapsulating the encapsulated data from said first encapsulating step in accordance with a second protocol(see col. 2, lines 9-25); wherein said first encapsulating step supplements a real data part including said data to be transmitted to said data receiving means with an additional information part associated with said real data part, said first encapsulating step further encrypting said real data part(see col. 5, lines 16-55).

18. As per claim 22, Aziz et al. discloses wherein said additional information part includes destination address information identifying the data receiving means authorized to receive data included in said real data part(see col. 3, lines 65-67, col. 4, lines 1-17).
19. As per claim 23, Aziz et al. discloses wherein said destination address information is either individual or group destination address information(see col. 4, lines 16-17).
20. As per claim 24, Aziz et al. discloses wherein said data transmitting means possesses session keys corresponding to said destination address information, said session keys being used by said data transmitting means to encrypt information and data and by said receiving means to decrypt the encrypted information and data received; and wherein said data transmitting means transmits in advance said session keys to the data receiving means authorized to receive the transmitted information and data in accordance with said destination address information(see col. 9, lines 59-67, col. 10, lines 1-15, 46-54, 64-67).
21. As per claim 25, Aziz et al. discloses wherein said session keys are updated at predetermined intervals(see col. 16, lines 46-65).
22. As per claim 26, Aziz et al. discloses wherein said session keys are transmitted over a communication channel permitting either unidirectional communication from said data transmitting means to said data receiving means or bi-directional communication there between(see col. 10, lines 1-9).
23. As per claim 27, Aziz et al. discloses wherein said first encapsulating step uniquely determines how said destination address information attached to said real data part is stored into said additional information part, said first encapsulating step further encrypting said real data

part using a master key specific to the data receiving means corresponding to said destination address information(see col. 10, lines 32-39, 46-54, 64-67).

24. As per claim 28, Aziz et al. inherently discloses wherein said additional information part provides a 48-bit space in which to accommodate said destination address information(see fig. 10, sheet 6, col. 6, lines 41-43).

25. As per claim 29, Aziz et al. discloses wherein said first encapsulating step encapsulates the data to be transmitted to said data receiving means in accordance with either the Internet protocol or the Ethernet protocol (see col. 6, lines 55-61).

26. As per claims 30-31, 36-37, wherein said data receiving means is constituted as an IP router, and a bridge(see col. 1, lines 64-67, col. 2, lines 1-8).

27. As per claims 32-33, 35, Aziz et al. discloses controlling transmission of data from data transmitting means to data receiving means over communication channels and for causing said data transmitting means to encrypt data and transmit the encrypted data to said data receiving means over said communication channels(see col. 1, lines 64-67, col. 2, lines 1-8), said data transmission controlling method comprising the steps of encrypting data using an encryption key; supplementing the encrypted data with encryption key information about said encryption key; transmitting said encrypted data together with said encryption key information from said data transmitting means to said data receiving means; and decrypting said encrypted data using one of a plurality of decryption keys which allow said data receiving means to decrypt said encrypted data and which are updated frequently, said one of the decryption keys being selected in accordance with said encryption key information attached to said encrypted data(see col. 2, lines 9-45, col. 9, lines 14-15, 20-22, 45-55).

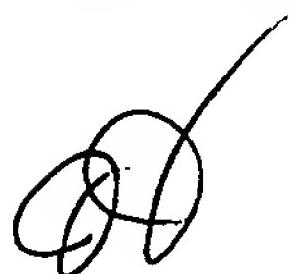
28. As per claim 34, Aziz et al. discloses wherein said encryption key and said decryption keys are session keys for encrypting information and data(see col. 9, lines 14-15, 45-55, 59-67, col. 10, lines 1-9).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (703) 306-0426. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-0040 for regular communications and (703) 308-6306 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.



September 8, 2003



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100